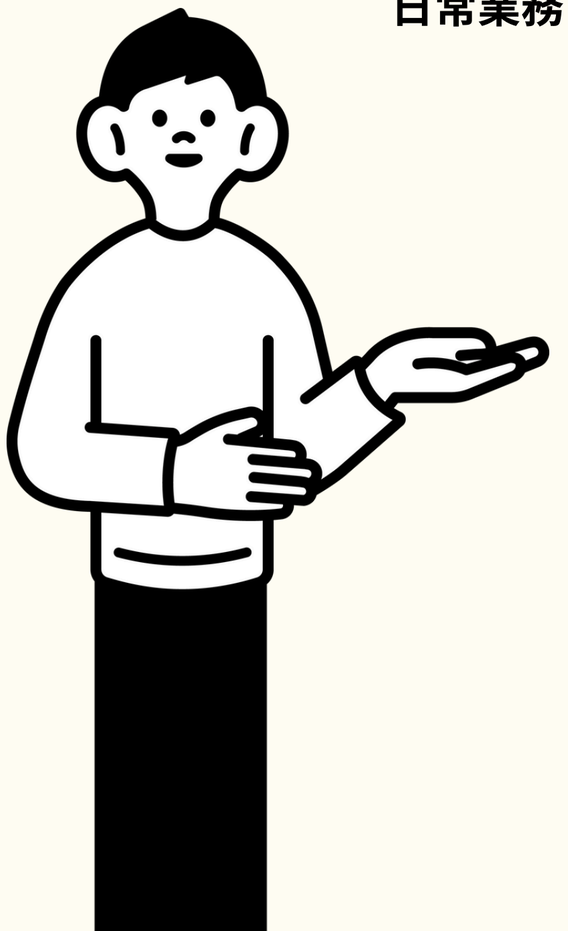
NTT docomo Solutions

セキュリティ教育通信
2025年8月号

NTTドコモソリューションズ株式会社

8月の
セキュリティ教育テーマ



日常業務で起こりやすい3つのセキュリティリスクについて、シンプルにわかりやすく学んでいきます。
1つ1つのテーマで『なぜ危ないのか』『どう防ぐか』を具体的に紹介していきます。

1 基本対策｜Basic Countermeasures
禁止された端末での業務利用によるリスクと責任

2 インターネットの脅威｜Online Threats
Webプッシュ通知を悪用した攻撃に注意

3 季節・社会動向の注意点｜Seasonal Security
ソーシャルエンジニアリング（電話での情報聞き出し）

１．禁止された端末での業務利用によるリスクと責任

その1回が、あなたの責任になるかもしれません

その端末、本当に“使っていい”ものですか？

許可されていない端末でログイン。
情報漏えい時に責任が問われることも。

１．禁止された端末での業務利用によるリスクと責任

“会社が守れる環境”で業務をすることが、一番確実な防御です

許可されている端末

- ログや操作履歴が残る
- セキュリティ対策済み
- 紛失時にリモートロック可能
- 利用がルール内で安心

許可されていない端末

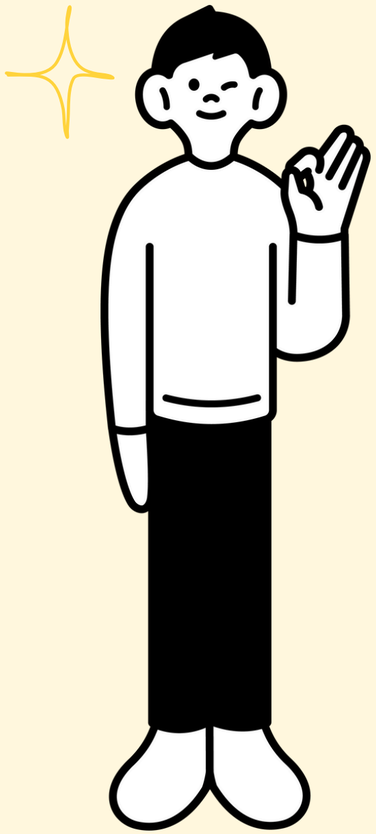
- 操作の記録が残らず、調査不能に
- ウイルス感染や情報流出のリスク大
- データが抜かれても止められない
- 利用者に責任が問われる可能性あり

業務アカウントは、許可された端末のみで使うことを徹底しましょう

１．禁止された端末での業務利用によるリスクと責任

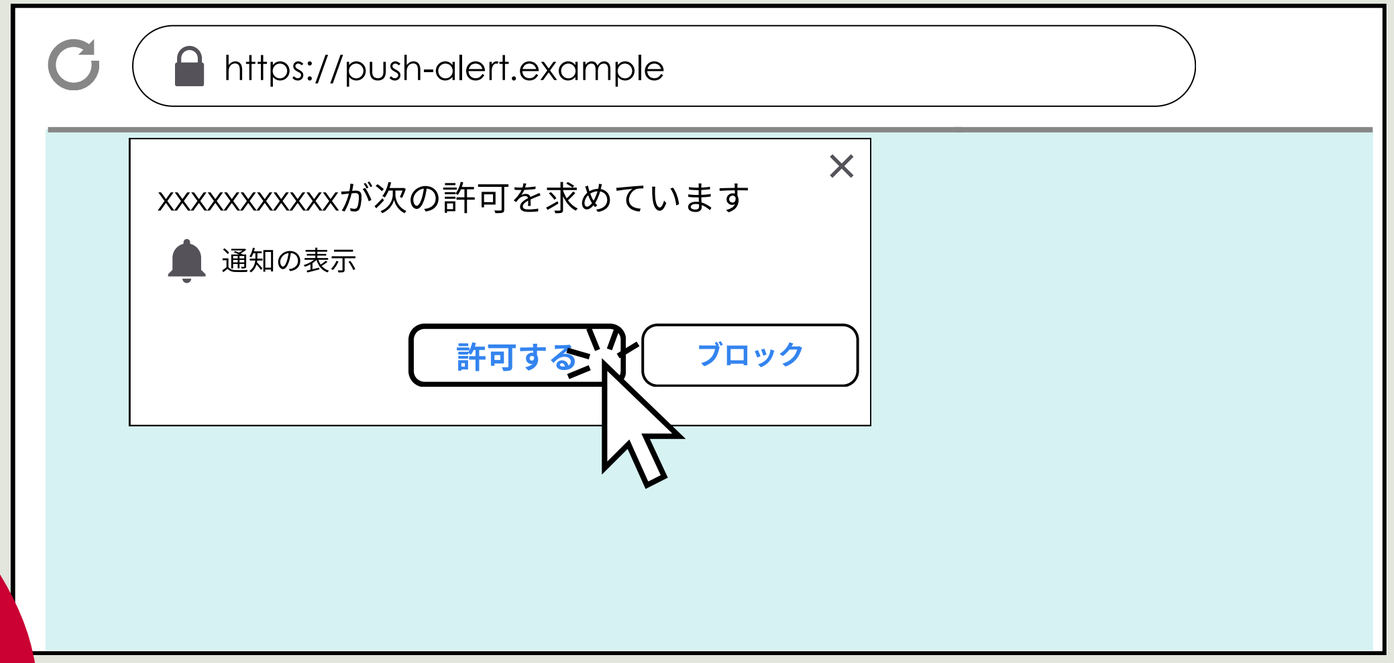
“やってるかも...”と思ったら、今日から見直しを！

行動	YES/NO
未許可のPCで業務メールを開いたことがある	□ / □
自分のスマホから資料をダウンロードした	□ / □
家族が使うタブレットで社内チャットを確認した	□ / □
どの端末が“許可されているか”正直よく知らない	□ / □



２．Webプッシュ通知を悪用した攻撃に注意

たった1クリックで、攻撃は始まる。

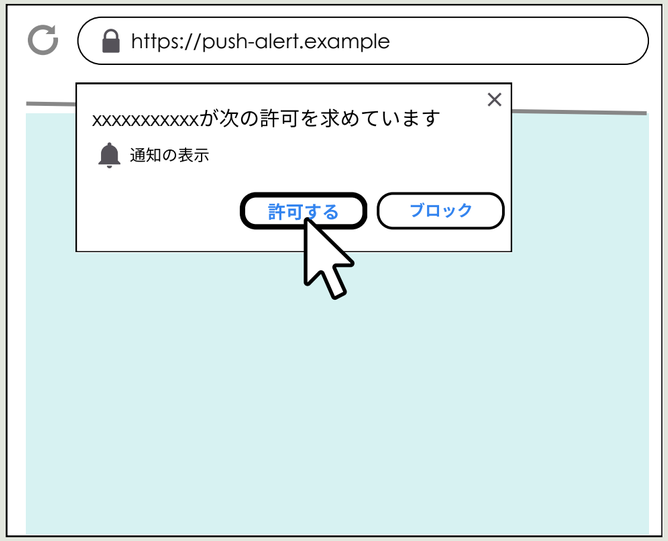


…通知を「**許可**」した“その瞬間”、
だましの仕掛けは動き出します！

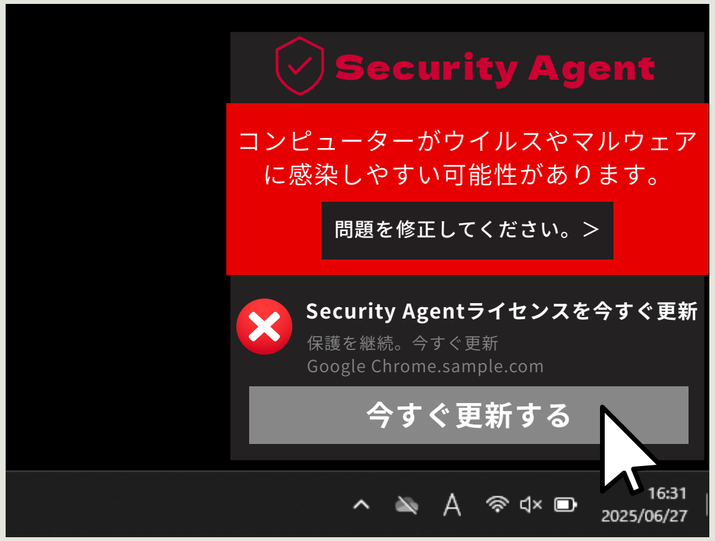
２．Webプッシュ通知を悪用した攻撃に注意

「通知を許可」しただけで始まる、巧妙な詐欺の流れとは？

1 ウェブサイト上でブラウザの通知を許可するよう要求



2 ブラウザ起動中に偽の通知が表示される



3 通知表示をクリックすると不審なサイトへ誘導

＜対策＞

１．「通知の許可」は基本“ブロック”（業務で必要なケースは少数）
２．不用意に“許可”を押さない習慣を！
３．許可した覚えがないのに通知が届いた場合は、IT管理部門へ連絡

２．Webプッシュ通知を悪用した攻撃に注意

あなたは大丈夫？通知詐欺に引っかからない3つの確認

Q1. ウェブサイトで「通知の許可を求めるメッセージ」が表示されたとき、どう対応すべき？

１．よく使うサイトなら、念のため許可しておく

２．必要性がない限り、通知はブロックする

３．とりあえず許可して、あとで考える

Q2. 「ウイルスに感染しています」という通知が突然出たら？

１．すぐ通知をクリックして指示に従う

２．念のためPCを再起動する

３．通知は無視して、上司や周りに相談する

Q3. 攻撃者が“通知”を悪用して狙っているのは？

１．偽サイトに誘導して不正アクセスや情報搾取をすること

２．システムをアップデートさせるため

３．利便性を高める新機能の案内

「通知」は“便利”と“危険”が紙一重。
クリック前に「本当に必要？」を問いかけるクセを！

正解：Q1.２　Q2.３ Q3.１

季節・社会動向の注意点｜Seasonal Security

３．ソーシャルエンジニアリング（電話での情報聞き出し）

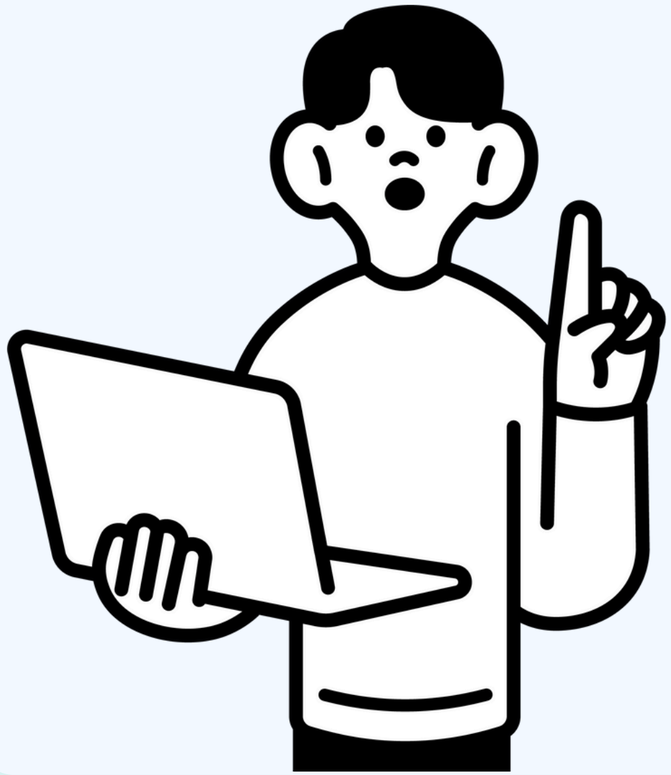
巧妙化する“なりすまし電話”
その対応ちょっと待って！

「情報システム部の○○ですが…」
あなたの“親切心”が、重大な漏えいのきっかけに。

３．ソーシャルエンジニアリング（電話での情報聞き出し）

ソーシャルエンジニアリングとは？

人の“うっかり”や“親切心”を悪用して、大事な情報を盗み出す手口のことです。



電話でIDやパスワードを聞かれたら ― 必ず断る！

攻撃者は以下のように装ってきます！

- 社内のシステム管理者や上司の“なりすまし”
- 「緊急対応が必要」と焦らせてくる
- 実在するプロジェクト名などで信頼を得ようとする

社員として取るべき対策

- ☑ 「電話では絶対に認証情報を教えない」ことを徹底
- ☑ 誰からの電話か分からないときは、正規の連絡手段で確認する習慣を持つ
- ☑ 「急いでいる」「困っている」と言われても、安易に信じず一呼吸置く

⚠ **実例：2023年、愛知県の企業で電話によるなりすまし被害が発生。**
管理者を装う相手にID・パスワードが漏洩。

３．ソーシャルエンジニアリング（電話での情報聞き出し）

電話・会話から始まる“だまし”に備えよう！(確認チェック)

Q. ソーシャルエンジニアリングとは何ですか？

A. セキュリティ機器の故障

B. 人の心理を突いて情報をだまし取る手口

C. 工場の生産工程に関する仕組み

Q.「情報システム部の○○ですが…」という電話がかかってきた。
IDとパスワードを聞かれた場合、どう対応すべき？

A. 相手の名前を聞いて教える

B. 社内の人なら教えて問題ない

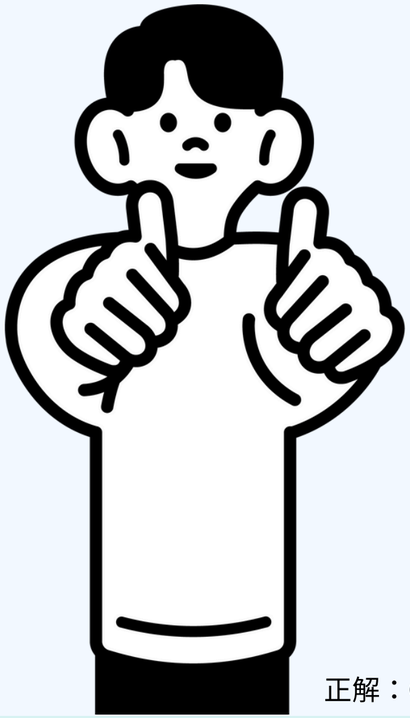
C. 認証情報は絶対に教えず、正規の連絡手段で確認する

Q. 攻撃者が“電話”を使う理由として正しいものは？

A. 文書より証拠が残りやすいから

B. 音声はセキュリティ的に安全だから

C. 相手を焦らせて判断を鈍らせやすいから



正解：Q1.B Q2.C Q3.C